decrypting said message with said integrated decryption circuit; and

deleting said private cypher key from said receiver's communication device.

24. (New) An apparatus of encrypting and decrypting Internet, Intranet, and E-mail messages, comprising:

a communication device;

an integrated circuit in communication with said communication device;

a random private cypher key generator embedded within said integrated circuit;

asymmetric encryption and decryption algorithms embedded within said integrated circuit; and

symmetric encryption and decryption algorithms embedded within said integrated circuit.

25. (New) The apparatus of claim 24 wherein said integrated is capable of password protection, thereby requiring a password to access said integrated circuit.

26. (New) The apparatus of claim 24 wherein said password is user defined.

Remarks

Responsive to the Office Action mailed March 22, 2001, the Applicant submits this amendment. In this Amendment, claims 1-6 have been canceled, claim 7 has been amended, and claim 8-26 have been added. Applicant notes with appreciate the Examiner has indicated claim 7 would be allowable if re-written in accordance with

35 USC §112. Reconsideration of the present application in view of the changes set forth above is hereby requested.

Objection to Drawings

In the aforementioned Office Action, the Examiner has objected to the drawings under 37 CFR 1.84(p)(4), in that the reference number '56' has been used to designated both "send message through a private network" and "send message through network." Correction of the specification and drawing is included herewith.

In addition, the Examiner has objected to the drawings under 37 CFR 1.84(p)(5), in that "they do not follow the reference sign(s) mentioned in the description 30, 32, 34, 36, and 38. A corrected substitute drawing is included herewith.

In addition, the Examiner has objected to the drawings under 37 CFR 1.84(p)(5), in that "they include reference sign(s) not mentioned in the 10, 12, 14, 16, and 18. Correction of the specification is included herewith.

Rejections under 35 USC §112

Claims 3-7 have been rejected under 35 USC §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention. Applicant has cancelled claims 1-6, and amended claim 7. By the above amendment it is respectfully submitted that all claims present in the application are in full compliance with 35 USC §112, second paragraph. Applicant notes that such amendments are not intended to limit the claimed invention. Rather, such amendments are being made solely in response to Examiner's rejection under 35 USC §112.

Rejections under 35 USC §103

In the above-referenced Office Action, the Examiner rejected claims 1-6 under 35 USC §103 in light of Hice et al.

As claims 1-6 have been canceled by this amendment, the Applicant respectfully submits the rejection is moot. The Applicant earnestly solicits allowance of the pending claims.

Conclusion

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached page is captioned "**Version with markings to show changes made**."

Therefore, it is submitted that all pending claims 7-26 are in condition for immediate allowance, and such action is respectfully requested. However, if for any reason direct communication with Applicant's attorney would serve to advance prosecution of this application to finality, the Examiner is cordially urged to contact the undersigned attorney at the below listed telephone number.

Respectfully submitted,

Dated: July 23, 2001

Brian Swienton
Reg. No. P-49, 030

Brian Swienton, Esq.
Cyberdog Communication, Inc.
1833 Diamond St., Suite 201
San Marcos, CA 92069
(760) 744-8310 phone

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In The Claims:

Please amend claim 7 as follows:

7. (Amended) A method for efficient encryption and decryption of Internet, Intranet, or e-mail messages, comprising the steps of:

providing a sending unit in communication with an integrated encryption circuit embedded with an encryption algorithm;

encrypting a message at [a] said sending unit [which is to be sent to a receiving unit using an integrated circuit embedded with an algorithm located within said sending unit];

appending to the message at said sending unit [the] a receiver's unencrypted IP address;

appending to said message [the] a receiver's encrypted IP address;

[said sending unit sends] sending said encrypted message with said unencrypted IP address and said encrypted IP address to a receiving unit;

providing said receiving unit having an integrated encryption circuit embedded with an decryption algorithm;

[receiving unit with an integrated circuit embedded with an encryption algorithm located within said] receiving with said receiving unit said encrypted message with said unencrypted IP address and said encrypted IP address;

[receiving unit decrypts] decrypting with said receiving unit said encrypted IP address, thereby resulting in a decrypted IP address; [storing said decrypted IP address in a register built into said integrated circuit embedded encryption algorithm within receiving unit]

storing said decrypted IP address in a first register built into said integrated encryption circuit within receiving unit;

[receiving unit stores] storing said unencrypted IP address into a second register built into said integrated encryption circuit [embedded with an encryption algorithm located] within said receiving unit;

means for comparing said second register storing unencrypted IP address to said first register storing said decrypted IP address;

[receiving unit decrypts] decrypting said message if said second register storing unencrypted IP address matches said first register storing said decrypted [encrypted] IP address; and

means for halting decryption process if said second register storing unencrypted IP address does not match said first register storing said decrypted [encrypted] IP address.

Please add new Claims 8-26 as follows:

8. (New) A method of encrypting Internet, Intranet, or e-mail messages, comprising:

providing a communication device in communication with a private encryption key generator;

generating a primary private encryption key;

encrypting data with said primary private encryption key;

providing a public encryption key and second private encryption key pair;

encrypting said primary private encryption key and with a public/second private encryption key pair; and

sending said data encrypted with said primary private encryption key and said primary private encryption key encrypted with said public/second private encryption key pair to a receiving unit.

9. (New) The method of claim 8, wherein access to said private encryption key generator is password controlled.

10. (New) The method of claim 9 wherein said password is user defined.

11. (New)The method of claim 8 wherein said encryption key generator is located within a communication device.

12. (New) The method of claim 8 wherein said primary private encryption key is randomly generated.

13. (New) A method of decrypting Internet, Intranet, or e-mail messages, comprising:

providing a communication device in communication with a private encryption key generator;

receiving an encrypted message with said communication device, said message having data encrypted with a primary private encryption key and a primary private encryption key encrypted with a public/second private encryption key pair;

providing access to said private encryption key generator;

decrypting said public/second private encryption key pair with said private encryption key generator. thereby providing said primary private encryption key; and

decrypting said data with said primary private encryption key.

14. (New) The method of claim 13 wherein access to said private encryption key generator is password controlled.

15. (New) The method of claim 14 wherein said password is user defined.

16. (New) The method of claim 13 wherein access to said primary encryption key generator is requires verification.

17. (New) The method of claim 16 wherein said verification comprises a Certification of Authority.

18. (New) A method of encrypting Internet, Intranet, or e-mail messages, comprising the steps of:

providing a communication device in communication with an integrated encryption circuit embedded with encryption algorithms;

accessing said integrated encryption circuit to encrypt a message;

encrypting said with said encryption algorithms;

providing a message header comprising a sender's private cypher key and a digital bit array;

encrypting said message header using a receiver's public encryption key;

appending said encrypted message header to said encrypted message; and

transmitting said encrypted message header and said encrypted message to a receiver.

19. (New) The method of claim 18 wherein said message is transmitted through an Internet.

20. (New) The method of claim 18 wherein said message is transmitted through an Intranet.

21. (New) The method of claim 18 wherein said message is transmitted through an e-mail.

22. (New) The method of claim 18 wherein said message is transmitted through a wireless communication system.

23. (New) A method decrypting a message of claim 18 further comprising the steps of:

providing a communication device in communication with a integrated decryption circuit;

receiving an encrypted message and encrypted message header with said communication device;

accessing said integrated decryption circuit to decrypt said encrypted message and message header;

decrypting said message header with said decryption circuit;

validating said message header with said decryption circuit;

decrypting said message with said integrated decryption circuit; and

deleting said private cypher key from said receiver's communication device.

24. (New) An apparatus of encrypting and decrypting Internet, Intranet, and E-mail messages, comprising:

a communication device;

an integrated circuit in communication with said communication device;

a random private cypher key generator embedded within said integrated circuit;

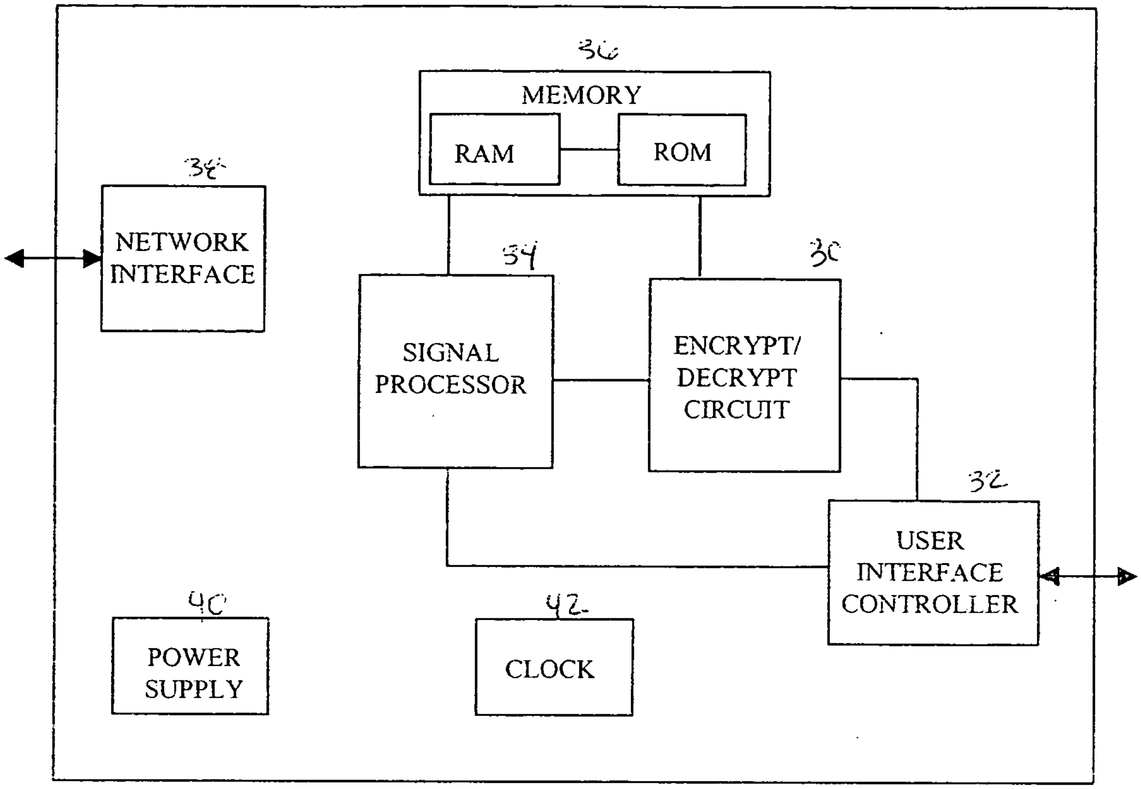

FIGURE 3 of 4 ENCRYPTION/DECRYPTION COMMUNICATION DEVICE

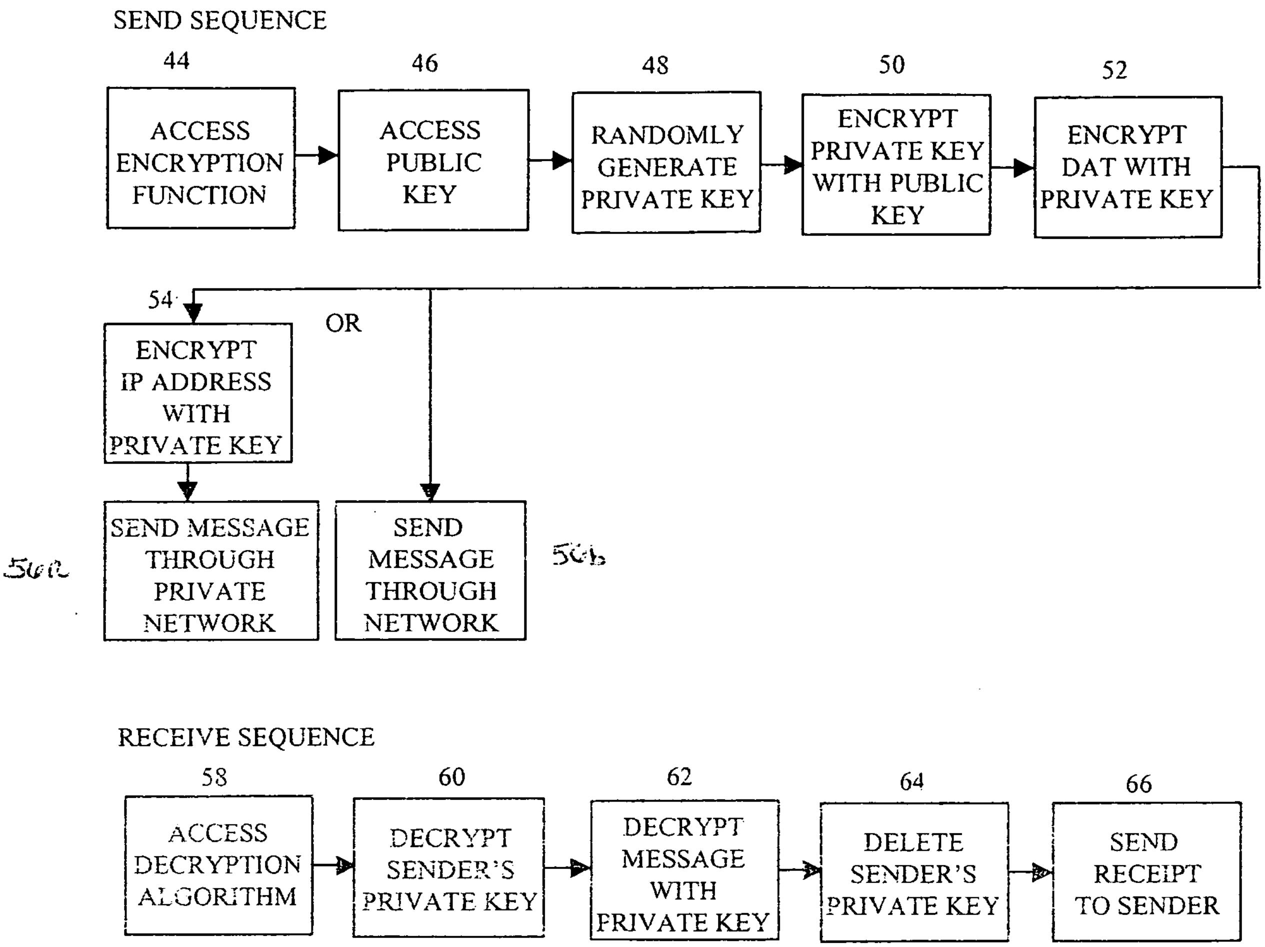
SEND SEQUENCE
44
ACCESS ENCRYPTION FUNCTION
46
ACCESS PUBLIC KEY
48
RANDOMLY GENERATE PRIVATE KEY
50
ENCRYPT PRIVATE KEY WITH PUBLIC KEY
52
ENCRYPT DAT WITH PRIVATE KEY
54
ENCRYPT IP ADDRESS WITH PRIVATE KEY
OR
56a
SEND MESSAGE THROUGH PRIVATE NETWORK
SEND MESSAGE THROUGH NETWORK
56b
RECEIVE SEQUENCE
58
ACCESS DECRYPTION ALGORITHM
60
DECRYPT SENDER'S PRIVATE KEY
62
DECRYPT MESSAGE WITH PRIVATE KEY
64
DELETE SENDER'S PRIVATE KEY
66
SEND RECEIPT TO SENDER

FIGURE 4 of 4 ENCRYPTION/DECRYPTION FLOW